Claims:

Following is a complete listing of the claims pending in the application:

1. (Original) A method of registration, comprising:

receiving a hash of a public key and a written signature of each of a plurality of registrants through a first channel of communications that includes hand-delivery;

receiving a public key and associated identifying information of at least some of the plurality of registrants through a second channel of communications, different from the first channel of communications that excludes hand-delivery;

B1 for each of the plurality of registrants, digitally signing the public key if the hash of the public key of the registrant received through the first channel of communications corresponds to the public key of the registrant received through the second channel of communications; and

providing the digitally signed public keys to an authenticating authority.

2. (Original) The method of claim 1, further comprising:

rejecting the registrant if the hash of the public key of the registrant received through the first channel of communications does not correspond to the public key of the registrant received through the second channel of communications.

3. (Original) The method of claim 1 wherein receiving a hash of a public key and a written signature through a first channel of communications includes receiving a written message via a courier.

4. (Original) The method of claim 1 wherein receiving a public key and associated identifying information through a second channel of communications includes detecting a signal carried in at least one of an electrical, a magnetic, and an electro-magnetic carrier.

5. (Original) The method of claim 1 wherein the hash of the public key and the written signature of the registrants received through the first channel of communications are non-electronic.

6. (Original) The method of claim 1, further comprising:

providing each of the registrants a copy of the respective digitally signed public key.

7. (Original) The method of claim 1, further comprising:

creating a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

8. (Original) The method of claim 1, further comprising:

enabling the registrants to submit the public key and associated identifying information through the second channel of communications only after receiving the hash of the public key and written signature through the first channel of communications.

9. (Original) The method of claim 1, further comprising:

preventing the registrants from submitting the public key and associated identifying information through the second channel of communications until after the hash of the public key and written signature are received through the first channel of communications.

10. (Original) The method of claim 1, further comprising:

entering the hash of the public key received though the first channel of communications into an electronic database.

11. (Original) A computer-readable medium whose contents cause a computer to register voter registrants by:

for each of a plurality of voter registrants, electronically receiving a hash of a public key that was transmitted by the registrant through a first channel of communications including hand-delivery;

for each of at least some of the plurality of voter registrants, electronically receiving a public key and associated identifying information that was transmitted by the voter registrant through a second channel of communications excluding hand-delivery;

for each of a number of the voter registrants, digitally signing the respective public key of the registrant if the hash of the public key received from the voter registrant corresponds to the public key received from the voter registrant; and

providing the digitally signed public keys to an authenticating authority.

12. (Original) The computer-readable medium of claim 11 whose contents further cause the computer to register voter registrants by:

creating a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

13. (Original) A voter registration computer system, comprising:

a public key hash input subsystem that for each of a plurality of voter registrants, electronically receives a hash of a public key that was transmitted by the voter registrant through a first channel of communications including hand-delivery;

a public key input subsystem that, for each of at least some of the plurality of voter registrants, electronically receives a public key and associated identifying information transmitted by the voter registrant through a second channel of communications excluding hand-delivery;

a digital signature subsystem that, for each of a number of the voter registrants, digitally signs the respective public key of the voter registrant if the hash of

the public key received from the voter registrant corresponds to the public key received from the voter registrant; and

a digitally signed public key output subsystem that provides the digitally signed public keys to an authenticating authority.

14. (Original) The voter registration computer system of claim 13, further comprising:

a hashing subsystem that creates a hash of the public key received through the second channel of communications for comparison to the hash of the public key received through the first channel of communications.

15. (Original) A method of voter registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public key through a first channel of communications including hand-delivery and that submitted the public key corresponding to the hash through a second channel of communications excluding hand-delivery; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

16. (Original) The method of claim 15 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

17. (Original) A computer-readable medium whose contents cause a computer to register voter registrants by:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public key through a first channel of communications including hand-delivery and that submitted the public key

corresponding to the hash through a second channel of communications excluding hand-delivery; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

18. (Original) The computer-readable medium of claim 17 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

19. (Original) A voter registration computer system, comprising:

an input subsystem that receives a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that submitted a hash of the public key through a first channel of communications including hand-delivery and that submitted the public key corresponding to the hash through a second channel of communications excluding hand-delivery; and

an authentication subsystem that authenticates a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

20. (Original) The voter registration computer system of claim 19 wherein the public key encrypted votes are digitally signed by the respective voter registrants.

21. (Original) A method of registration, comprising:

receiving a respective public key for each of a plurality of registrants;

for each of at least some of the plurality of registrants, verifying an identity of the registrant in-person;

for each of the verified registrants, receiving a signature of the registrant on a respective hash card including a written hash of the public key of the registrant;

for each of the verified registrants, digitally signing the public key received from the registrant if the hash on the hash card corresponds to the public key received from the registrant; and

providing the digitally signed public keys to an authenticating authority.

22. (Original) The method of claim 21, further comprising:

providing an acknowledged duplicate of the respective hash card to each of the verified registrants.

23. (Original) The method of claim 21, further comprising:

providing a copy of the respective digitally signed public key to each of the verified registrants.

24. (Original) The method of claim 21, further comprising:

rejecting the registrant if the hash on the hash card does not correspond to the public key received from the registrant.

25. (Original) The method of claim 21, further comprising:

providing a form for creating the hash card to at least some of the registrants.

26. (Original) The method of claim 21, further comprising:

providing a copy of public/private key pair generation software to at least some of the registrants.

27. (Original) The method of claim 21, further comprising:

prompting the registrants to generate the hash card; and

prompting the registrants to transmit the public key.

28. (Original) The method of claim 21 wherein identifying the registrant in-person includes at least one of comparing the registrant to a picture identification and comparing a signature of the registrant to a signature of the picture identification.

29. (Original) A computer-readable medium whose contents cause a computer to register registrants by:

receiving a respective public key for each of a plurality of registrants;

for each of at least some of the plurality of registrants, receiving an indication that an identity of the registrant has been verified in-person;

for at least a number of the verified the registrants, digitally signing the public key received from the registrant if a public key hash submitted by the registrant on a hash card including a written signature of the registrant corresponds to the public key received from the registrant; and

providing the digitally signed public keys to an authenticating authority.

30. (Original) The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

automatically producing an acknowledged duplicate of the respective hash card for each of the verified registrants.

31. (Original) The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

rejecting the registrant if the hash on the hash card does not correspond to the public key received from the registrant.

32. (Original) The computer-readable medium of claim 29 whose contents further cause the computer to register registrants, by:

automatically providing a web page form for creating the hash card to at least some of the registrants.

33. (Original) A registration computer system, comprising:

a public key input subsystem that receives a respective public key for each of a plurality of registrants;

a tracking subsystem that, for each of at least some of the plurality of registrants, receives an indication that an identity of the registrant has been verified in-person;

a digital signature subsystem that, for at least a number of the registrants indicated as having identities verified in-person, digitally signs the public key received from the registrant if a public key hash submitted by the registrant on a hash card including a written signature of the registrant corresponds to the public key received from the registrant; and

a digital signed public key output subsystem that provides the digitally signed public keys to an authenticating authority.

34. (Original) A method of voter registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that have had their identity verified in-person by the registrar and that have submitted a hash card to the registrar including a written signature and a public key hash corresponding a public key electronically submitted to the registrar by the registrant; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

35. (Original) A method of registration, comprising:

for each of a plurality of registrants, verifying an identity of the registrant in person;

for at least some of the plurality of registrants, producing a public/private key pair;

for each of a number of the voter registrants that have had their respective identities verified in person, digitally signing the public key of the respective produced public/private key pair;

providing the private key of the respective produced public/private key pair to each of the registrants that have had their respective identities verified in-person; and

providing the digitally signed public keys to an authenticating authority.

36. (Original) A method of registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants that have had their respective identities verified by the registrar in-person; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.

37. (Original) A method of registration, comprising:

electronically receiving a public key and associated identifying data from each of a plurality of registrants over at least one communications channel;

digitally signing each of the received public keys of the registrants whose identifying data is not the same as the identifying data of the other registrants; and

providing the digitally signed public keys to an authenticating authority.

38. (Original) The method of claim 37 wherein digitally signing each of the received public keys of the registrants whose identifying data is not the same as the identifying data of the other registrants includes comparing the identifying data of at least one of the registrants to the identifying data of at least another one of the registrants.

39. (Original) The method of claim 37 wherein electronically receiving a public key and associated identifying data includes receiving at least one of a registrant name, a registrant address and a unique registrant identifier.

40. (Original) A method of voter registration, comprising:

receiving a plurality of digitally signed public keys from a registrar, where each of the digitally signed public keys belongs to a respective one of a plurality of voter registrants having different identifying data from the other voter registrants; and

authenticating a number of public key encrypted votes received from at least some of the plurality of voter registrants using the received digitally signed public keys.